Hiding the Text in Image of Variable Size

Abdullah .H. Muhammad

University of Kirkuk , collage of education, physics department

Received 14 April 2014 ; Accepted 1 February 2015

ABSTRACT

Steganography is the art and science of hiding information into digital media for the purpose of identification, annotation, and copyright. In a way that prevents the outside observer from recognizing the present of hiding information. In the current research, a design and implementation for image's Steganography system based on Least Significant Bits mechanism was presented and discussed. The performance of the hiding text system was considered up to 1-bits, 2-bits. 4-bits hiding rate. A new adaptive Least-Significant Bit method was suggested, implemented and tested, that based on the idea of the substitution criteria. The result have indicating a good hiding performance.

Keywords: Least Significant Bit (LSB), Data embedding, , Steganography, MSE, PSNR,

اخفاء نص في صوره ذات حجم متغير

عبدالله حمود محمد

جامعة كركوك , كلية العلوم , قسم الفيزياء.

الخلاصة

الكتابة المغطاة(Steganography) هي فن وعلم إخفاء البيانات في الأوساط الرقمية بهدف حماية المعلومات الأمنية الهامة ,المطبوعات الرقمية وحقوق النشر بطريقة ما بحيث لا تسمح للغير بتمييز وجود معلومات مخفية داخل الأوساط الرقمية .الطرق الأكثر استخداما في ملفات (Least Significant Bit) في الإخفاء هي تقنية الإدراج في البت الأدنى

(Least 1-2-4bits)الصور الرقمية .هذا البحث تم فيه استخدام وتطبيق الإلية على اقل بتين معتمدين مبدأ التعويض . النتائج التي تم الحصول عليها من تطبيق هذه التقنية على النموذج أعطت قدرة وجودة على الإخفاء

الكلمات المفتاحيه: البت الاقل اهميه,تضمين البيانات,الاخفاء,متوسط مربع الخطا, نسبة الاشاره الى الضوضاء

INTRODUCTION

Steganography is a Greek work which means the covered writing. Steganography is an art of hiding data in a covered media (image, audio, video, text). In Steganography, we hide the mere presence of that it will be undetectable. The covered media is chosen in such a manner that it has capacity to hide the data and robustness that provides quality to the stego image[1]. As in the upcoming years the need of data hiding, copyright protection, and confidentiality increases, steganography plays an important role in this field because of its some unique features. In this paper, we focus on the different steganography methods. This section provides some important information about steganography methods that will help in future researches in steganography and data hiding field. This paper is divided into different sections in which we explain steganography system, related work, different steganography methods and conclusion.

RELATED WORK

In related work, LSB is the most common method used to hide the message developed by Chandramouli [2] by applying the filtering, masking and transformation on the cover object. LSB matching revisited image steganography and edge adaptive scheme to which can select the embedding region according to the size of secret data is proposed by

Weigi Luo [3]A.Hassan Mathkour [4] used a new image steganography scheme based on LSB replacement technique and pixel value differencing. Chen Ming [5] discussed different steganography algorithms and tools into spatial domain, transform domain, document based and other categories such as spread spectrum technique and video compressing encoding . Mankun Xu [6] proposed a model based steganography technique which is based on least square method to estimate the embedding rates of secret information. Anjali A. Shejul [7] proposed a DWT based approach for steganography using biometric features. Here, the secret data were embedded in skin region of image that provides secure location for data hiding. Secret data was hidden in one of the high frequency sub band of DWT by tracing skin pixels. All the steps of data hiding are applied on the cropped image. This provides security to the method and PSNR was used to determine the quality of stego image after embedding the secret data.

Physical Steganography

Physical Steganography has been widely used. In ancient time people wrote message on wood and then covered it with wax. Message was written on the back of postage stamps. Message was written on paper by secret inks[1].

Digital Steganography

Digital Steganography is the art of invisibly hiding data within data. It conceals the fact that message exists by hiding the actual message. In this, secret data can be hidden inside the image, text, sound clip which can be represented in binary[1].

Printed Steganography

Digital Steganography output can be in the form of printed documents. The letter size, spacing and other characteristics of a cover text can be manipulated to carry the hidden message. A recipient who knows the technique used can recover the message and then decrypt it[1].

Image Steganography

In this method, images are used as cover object. The image steganography, data hiding method can be classified into different categories. These are spatial domain, frequency domain, and adaptive domain[1].

Spatial Domain Steganography:

In spatial domain, cover image and secret data modified by using LSB and level encoding. First, the cover image is decomposed into bit planes and then LSB is of bit planes replaced with secret data fit. LSB substitution is the mostly used stenographic technique. This substitution concept includes embedding at the minimum weighting bit as it will not affect the value of original pixel. Luon Ching Lin [5] proposed a scheme of data hiding in spatial domain with tolerance of distortion. This method provides better image quality. The only drawback of the LSB insertion is the simplicity of extraction process. Thus, a secret listener can easily extract the data that we are sending .

Lsb Based Steganography

Algorithm to embed text message:-

Step 1: Read the cover image and text message which is to be hidden in the cover image.

Step 2: Convert text message in binary.

Step 3: Calculate LSB of each pixels of cover image.

Step 4: Replace LSB of cover image with each bit of secret message one by one.

Step 5: Write stego image

Algorithm to retrieve text message:-

Step 1: Read the stego image.

Step 2: Calculate LSB of each pixels of stego image.

Step 3: Retrieve bits and convert each 8 bit into character.

Evaluation of Image Quality:

For comparing stego image with cover results requires a measure of image quality, commonly used measures are Mean-Squared Error, Peak Signal-to-Noise Ratio and capacity.

Mean-Squared Error:

The mean-squared error (MSE) between two images I1(m,n) and I2(m,n) is: *M* and *N* are the number of rows and columns in the input images, respectively[8].

$$MSE = \frac{\sum_{x=1}^{M} \sum_{Y-1}^{N} [h(x,y) - f(x,y)]^2}{M.N}$$

also we can estimate the root mean square's error (RMSR) as follows

$$RMSR = MSE$$

Signal to Noise Ratio (SNR): A standard objective measure of coded image quality is signal-to-noise ratio (SNR) which is defined as the ratio between signal and reconstruction error variance [mean-square error (MSE)] usually expressed in decibels (dB) [8]:

$$\text{SNR (dB)} = 10 \log_{10}\left(\frac{\sum_{r=0}^{M-1}\sum_{c=0}^{N-1}\left[y(r,c)\right]^2}{\sum_{r=0}^{M-1}\sum_{c=0}^{N-1}\left[x(r,c) - y(r,c)\right]^2} \right)$$

$$= 10 \log_{10}\left(\frac{\sum_{r=0}^{M-1}\sum_{c=0}^{N-1}\left[y(r,c)\right]^2}{MSE} \right)$$

Peak Signal-to-Noise Ratio:

Peak Signal-to-Noise Ratio (PSNR) avoids this problem by scaling the MSE according to the image range[8]:

$$PSNR = 10\log_{10}\frac{256^2}{MSE}$$

PSNR is measured in decibels (dB). PSNR is a good measure for comparing restoration results for the same image.

The proposed method

LSB hiding technique (this program was made in (C# 2010 V) hide the secret text directly in the least one or two or four significant bits in the image pixels, hence that affect the image resolution, which reduce the image quality and make the image easy to attack. As well as this method is already has been attacked and broken. Therefore a new technique that able to make the secret message more secure and enhance the quality of the image is proposed. The proposed method hides the secret text based on searching about the identical values between the secret texts and image pixels. In this paper we use four size of cover image in order to see what is the influence of the image size on the fidelity criteria .

PERFORMANCE & RESULTS

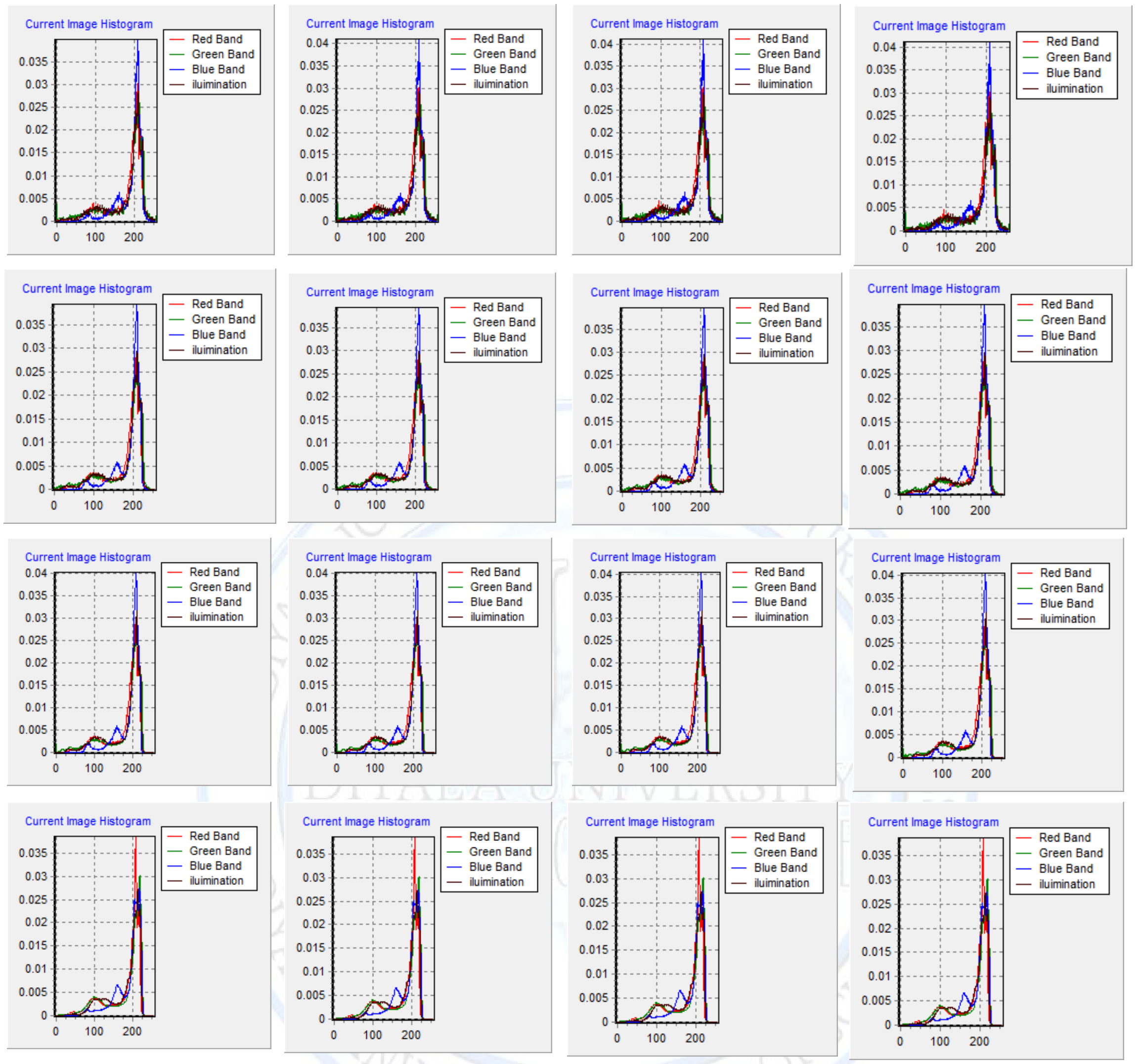
LSB based steganography embed the text message in LSB of cover image figure(6) and figure(7). This paper implements LSB based steganography, LSB based steganography and computes RMSE is root mean square's error and PSNR ratio. PSNR is the peak signal to noise ratio, in decibels, between two images(before and after hiding (1,2,3,4) . This ratio is used as a quality measurement between two images. If PSNR ratio is high then images are better of quality. Comparison of LSB based stego images using PSNR ratio shows that PSNR ratio of LSB based steganography scheme is high as compared to LSB based steganography scheme for all types of images as well as what we will see in the histogram of cover and strgo images figure(5). The PSNR value for the images is between (44-70).The PSNR value increases with the increase of the image size. The MSE value of the image is between (0.004-2.5). The MSE value decreases with the decrease of the image size. Peak signal to noise ratio is used to compute how well the methods perform. PSNR computes the peak signal to noise ratio, in decibels, between two images. This ratio is used as a quality measurement between two images. If PSNR ratio is high then images are best of quality as in table (1,2,3).

Figure(1) a-original image size 128, b-stego image with LSB1, c- stego image with LSB2 d- stego image with LSB4

Figure(2) a-original image size 256, b-stego image with LSB1, c- stego image with LSB2 d- stego image with LSB4

Figure(3) a-original image size 512, b-stego image with LSB1, c- stego image with LSB2 d- stego image with LSB4

Figure(4) a-original image size 1024, b-stego image with LSB1, c- stego image with LSB2 d- stego image with LSB4



Figure(5)

First-a-Histogram of original image size 128, b- Hist of stego image with LSB1,

c- Hist of stego image with LSB2 d- Hist of stego image with LSB4

First-a-Histogram of original image size 256, b- Hist of stego image with LSB1,

c- Hist of stego image with LSB2 d- Hist of stego image with LSB4

First-a-Histogram of original image size 512, b- Hist of stego image with LSB1,

c- Hist of stego image with LSB2 d- Hist of stego image with LSB4

First-a-Histogram of original image size 1024, b- Hist of stego image with LSB1,

c- Hist of stego image with LSB2 d- Hist of stego image with LSB4

Table (1): Results of embedded differential size image by using LSB1

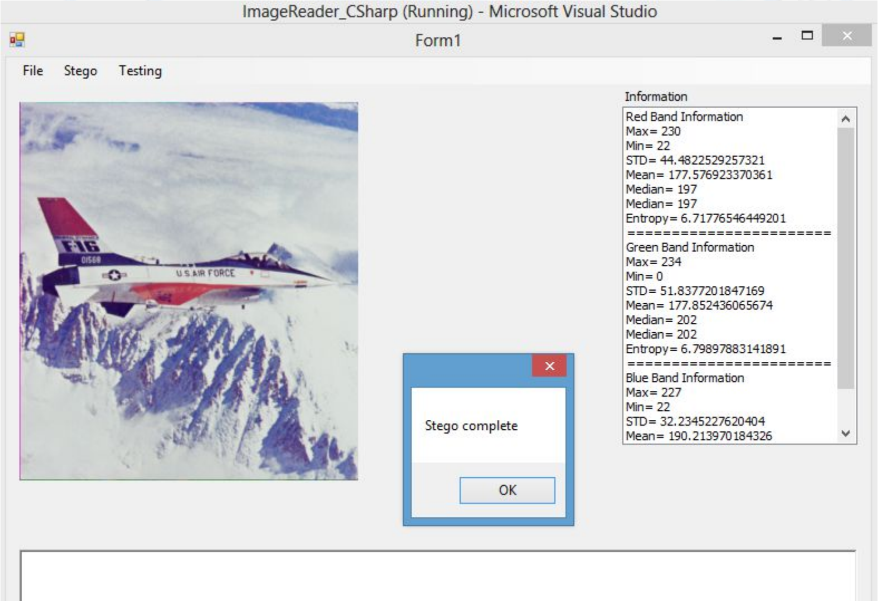
size	Mse R	Rmse R	Snr R	Psnr R
128	0.122619	0.350171	16.69786	57.2452
256	0.030075	0.173422	17.4322	62.7494
512	0.007359	0.085782	17.37273	68.5666
1024	0.001951	0.044173	16.34848	74.6284
size	**Mse G**	**Rmse G**	**Snr G**	**Psnr G**
128	0.119568	0.345786	17.5513	57.35466
256	0.030044	0.173333	17.43219	63.25035
512	0.007348	0.085715	17.81827	68.72315
1024	0.001769	0.04206	18.469	75.34126
size	**Mse B**	**Rmse B**	**Snr B**	**Psnr B**
128	0.117554	0.348611	19.26791	57.15158
256	0.030167	0.173685	18.79464	62.55185
512	0.007473	0.086446	18.99948	68.38557
1024	0.001925	0.043869	18.40833	74.5411

Table (2): Results of embedded differential size image by using LSB2

size	Mse R	Rmse R	Snr R	Psnr R
128	0.294433	0.542617	6.95398	53.44093
256	0.072204	0.268709	7.07967	58.94389
512	0.017822	0.1335	7.172945	64.7249
1024	0.004438	0.066621	7.187151	71.05927
size	**Mse G**	**Rmse G**	**Snr G**	**Psnr G**
128	0.281799	0.530807	7.44704	53.6314
256	0.070419	0.265366	7.437496	59.55109
512	0.019012	0.137886	6.885634	64.5939
1024	0.004884	0.069884	6.6901	70.931153
size	**Mse B**	**Rmse B**	**Snr B**	**Psnr B**
128	0.276367	0.525706	8.10567	53.439
256	0.071579	0.267542	7.9209	58.79926
512	0.018703	0.13676	7.59127	64.401297
1024	0.004681	0.068415	7.568867	70.68127

Table (3): Results of embedded differential size image by using LSB4

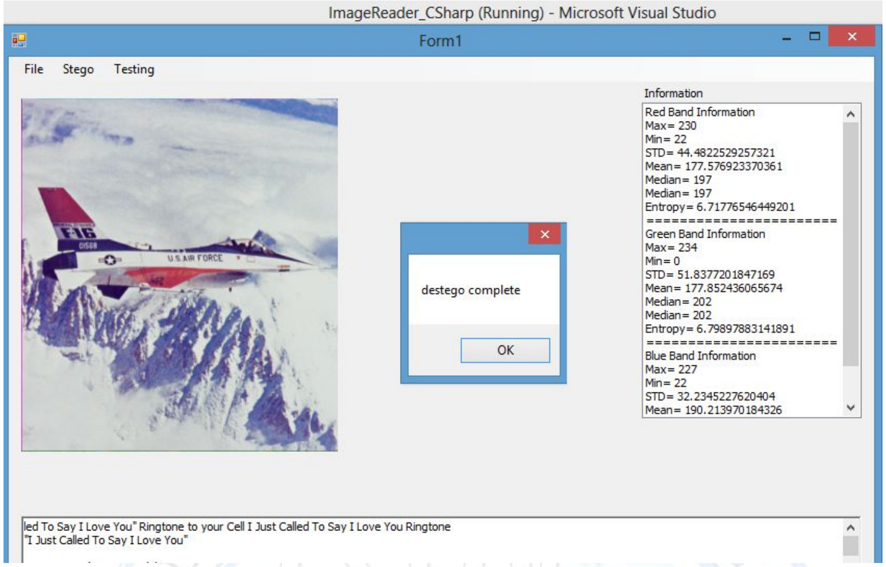
size	Mse R	Rmse R	Snr R	Psnr R
128	2..55358	1.597995	0.801807	44.05929
256	0.63949	0.79968	0.799356	49.47316
512	0.168731	0.41077	0.757642	54.96259
1024	0.041965	0.204855	0.760135	6.13E+08
size	**Mse G**	**Rmse G**	**Snr G**	**Psnr G**
128	2.353942	1.53425	0.891513	44.41284
256	0.611847	0.782206	0.856002	50.16158
512	0.156997	0.396229	0.833851	55.42538
1024	0.042811	0.206909	0.763181	61.50311
size	**Mse B**	**Rmse B**	**Snr B**	**Psnr B**
128	2.57666	1.605197	0.879051	43.74337
256	0.632858	0.795524	0.89588	49.33405
512	0.14185	0.376629	1.000941	55.60224
1024	0.033022	0.181722	1.072804	62.19617



Stego complete

```
Red Band Information
Max= 230
Min= 22
STD= 44.4822529257321
Mean= 177.576923370361
Median= 197
Median= 197
Entropy= 6.71776546449201
========================
Green Band Information
Max= 234
Min= 0
STD= 51.8377201847169
Mean= 177.852436065674
Median= 202
Median= 202
Entropy= 6.79897883141891
========================
Blue Band Information
Max= 227
Min= 22
STD= 32.2345227620404
Mean= 190.213970184326
```

Figure (6) Enter a Secret text to hide



```
Red Band Information
Max= 230
Min= 22
STD= 44.4822529257321
Mean= 177.576923370361
Median= 197
Median= 197
Entropy= 6.71776546449201
========================
Green Band Information
Max= 234
Min= 0
STD= 51.8377201847169
Mean= 177.852436065674
Median= 202
Median= 202
Entropy= 6.79897883141891
========================
Blue Band Information
Max= 227
Min= 22
STD= 32.2345227620404
Mean= 190.213970184326
```

```
led To Say I Love You" Ringtone to your Cell I Just Called To Say I Love You Ringtone
"I Just Called To Say I Love You"
```

Figure (7) make destego image

References

1. Rakhi1, Suresh Gawande. , "Audio steganography using bit modification", International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering,Vol. 2, Issue 10, October 2013
2. N. F. Johnson, S. Jajodia, "Exploring Steganography: Seeing the Unseen", IEEE Computer vol. 31, issue 2, pp. 26-34, 1998.
3. J. C. Judge, "Steganography: Past, Present, Future", SANS Institute Publications, 2001.
4. D.Artz, "Digital Steganography: Hiding Data within Data", Internet Computing IEEE, vol. 5, issue 3, pp. 75-80, 2001.
5. L-C. Lin, "Hiding Data in Spatial Domain with Distortion Tolerance", Computer Standard & Interfaces 31, pp. 458-464, (2009).
6. K. Gopalan. , "A REVIEW ON STEGANOGRAPHY METHODS", IEEE International Conference on Acoustics, Speech, and Signal Processing,(ICASSP '03), vol 2, pp. 6-10, April 2003.

7. Anjali A. Shejul, Prof. U. L. Kulkarni, “A DWT based Approach for Steganography using Biometric”, International Conference On Data Storage and Data Engineering, IEEE, pp. 39-43, 2010.

8. H. Sheisi, J. Mesgarian, and M. Rahmani “Steganography: Dct Coefficient Replacement Method and Compare With JSteg Algorithm “,International Journal of Computer and Electrical Engineering, Vol. 4, No. 4, August 2012